Proceedings of the 4th International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2026.33331

Research on the Standardized Operation of Sampling Evidence Collection Proof for Telecommunication Network Fraud

Mengxiao Kong

College of Humanities and Social Development, Northwest A&F University, Xianyang, China
397045406@qq.com

Abstract. The evidence in telecommunications and online fraud cases is increasingly going overseas in terms of quantification and dispersion, and the traditional model of evidence collection is difficult to meet the needs of judicial practice. Sampling evidence, with its efficiency, has become an important way to solve the problem of obtaining evidence in such cases, but it has encountered multiple practical obstacles: improper evidence collection procedures, formalistic cross-examination, and the absence of evidence review rules seriously restrict the actual effectiveness of sampling evidence. In view of this, a standardized sampling operation process should be established, an equal cross-examination mechanism between the prosecution and the defense should be improved, and hierarchical evidence certification rules should be established, with the aim of promoting the standardization of the application of sampling evidence and providing theoretical references for the precise determination and fair adjudication of such cases.

Keywords: telecommunication and Internet fraud, sampling evidence collection, criminal proof Introduction

1. Introduction

Telecom and Internet fraud crimes continue to occur frequently, and the modus operandi is constantly evolving. Investigation authorities face problems such as a large number of victims and scattered evidence in the evidence collection process. If the traditional model of verification and proof is still used, it will not only consume a large amount of judicial resources, but also lead to a mismatch between crime, responsibility and punishment.

In this context, sampling for evidence was introduced with the aim of solving the predicament of obtaining massive amounts of evidence and improving the efficiency of criminal justice [1]. Existing studies have mostly focused on the technical attributes of sampling evidence collection [2], normative basis [3], probative force review [4], etc., emphasizing a specific link of evidence collection or cross-examination, and not closely related to the characteristics of cases of telecommunications and online fraud. There is a lack of systematic review of the specific operational dilemmas.

DOI: 10.54254/2753-7048/2026.33331

Based on this, this paper takes the standardized operation of sampling evidence collection for telecommunications and Internet fraud as the core of the research, combines statistical principles, and proposes corresponding standardized paths for the predicaments it faces in the entire chain of evidence collection, cross-examination, and certification, to improve the criminal proof application system of sampling evidence collection and contribute to the improvement of the quality and efficiency of handling telecommunications and Internet fraud cases and the realization of judicial justice.

2. The connotation of sampling evidence collection for telecommunications and internet fraud

2.1. The concept of sampling evidence collection for telecommunications and internet fraud

The emergence of mass economic crimes such as telecommunications and Internet fraud in the information age has revealed the drawbacks of the traditional comprehensive evidence collection model. Sampling for evidence collection, as a new type of evidence collection method, has increasingly shown its advantages. As early as 1996, Article 37, Paragraph 2 of the Administrative Penalty Law stipulated that "when collecting evidence, administrative authorities may adopt the method of sampling for evidence collection" [5]. With the emergence of mass cases such as intellectual property infringement cases, sampling for evidence collection has also gradually appeared in the criminal field.

The mainstream view holds that In cases of telecom fraud involving massive amounts of evidence, investigation authorities use statistical principles to extract a portion of homogeneous evidence as sample evidence for observation and analysis, and make reliable estimates and inferences through indicators such as the quantity and proportion of sample evidence. A method of evidence collection for recognizing the overall homogeneity of evidence [6]. This approach is not a negation of the principle of comprehensive evidence collection. Instead, it is an optimized adaptation of the evidence collection model in the context of massive amounts of evidence in telecommunications and online fraud cases. By replacing individual verification with scientific sampling and compensating for the practical limitations of comprehensive evidence collection with statistical inference, it meets the practical needs of combating crime while also taking into account the rational allocation of judicial resources.

2.2. Legal characterization of sampling evidence collection in telecommunications and Internet fraud cases

At present, the normative characterization of sampling evidence collection in theory is mainly divided into two viewpoints: one is the "new proof method" theory [7]; The other is the "presumption that can be refuted" theory [8]. In fact, the evidence obtained through sampling does not fall into either of the two categories, but rather is a matter of the reliability of the expert opinion.

2.2.1. Telecommunications network fraud sampling evidence collection does not fall under "new proof methods"

Some academic views view sampling as a "new proof method" independent of traditional proof rules, but this positioning does not fit into the judicial logic of telecommunications and Internet fraud cases.

First, in terms of the proof mechanism, the so-called "new proof method" emphasizes the construction of a completely new factual determination path, while the sampling evidence collection

DOI: 10.54254/2753-7048/2026.33331

for telecommunications and Internet fraud does not deviate from the basic framework of the existing proof system. At its core is to infer the overall facts through the scientific analysis of sample evidence. Essentially, it still needs to follow the basic requirements of the three characteristics of evidence and be consistent with the value goals of traditional proof methods.

Secondly, the sampling and evidence collection in cases of telecommunications and online fraud focuses on the verification of a vast amount of evidence, which is merely a technical means for evidence collection and review, and has not created new proof rules. Finally, the reliability of its conclusion depends on the scientific nature of the sampling method and the normativity of the procedure, rather than the subversion of traditional proof logic and the definition of it as a "new proof method", which confuses the boundary between the means of evidence collection and the proof method.

2.2.2. The sampling of evidence for telecommunications and online fraud does not fall under "refutable presumption"

Refutable presumption centers on the empirical connection between the underlying facts and the facts to be proved [9], allowing the defense to overturn the presumption conclusion through counter-evidence, which is essentially different from the rule of sampling evidence for telecommunications and Internet fraud.

First, the presumption relies on empirical rules and normal connections. For example, the presumption of "providing technical support knowing that others are committing telecom and Internet fraud" is based on empirical judgment of behavioral patterns, while the sampling of telecom and Internet fraud is premised on the homogeneity of evidence, achieving an objective reflection of the whole through scientific sampling without relying on empirical connections, and has stronger objectivity and scientificity.

Secondly, the rebuttable presumption focuses on the logical deduction of "basic facts - presumed facts", and counter-evidence can directly deny the validity of the presumption, while in the case of telecommunications and Internet fraud sampling evidence, the defense can only raise objections regarding the sampling procedure and sample representativeness, and cannot directly deny the conclusion through simple counter-evidence [10]. Finally, the conclusions of sampling and evidence collection need to rely more on scientific methods to ensure reliability, so they should not be classified as refutable presumptions.

2.2.3. The sampling of evidence for telecommunications and online fraud should be regarded as an expert opinion

First of all, sampling and evidence collection should apply statistical expertise to analyze and judge the specialized issues in telecommunications and Internet fraud cases, which conforms to the core definition of the expert opinion "using science and technology or expertise to solve specialized problems" [11].

Secondly, the sampling and evidence collection of telecommunications and Internet fraud should be carried out by personnel with professional capabilities, and a written report should be formed, stating the basis, methods and results of the sampling, which is highly consistent with the formal requirements and procedural requirements of the expert opinion. The conclusion can directly prove the sentencing facts such as the amount of crime, or indirectly support the core facts. It needs to be comprehensively determined in combination with the evidence of the entire case and is in line with the proof function of the expert opinion. Finally, defining the conclusion of sampling evidence

DOI: 10.54254/2753-7048/2026.33331

collection for telecommunications and online fraud as an expert opinion is in line with its essential attributes and can provide a clear legal positioning for judicial practice.

2.3. Conditions for the application of sampling evidence collection for telecommunications and Internet fraud

The application of sampling for evidence collection in cases of telecommunications and Internet fraud is not a random choice of evidence collection method, but requires meeting the three core prerequisites of necessity, homogeneity and feasibility, which are interlinked and together constitute the basis for the legal application of sampling for evidence collection [12].

Necessity is the primary prerequisite for the application of sampling evidence, and the core criterion is that the amount of evidence is particularly large and it is indeed impossible to collect each one due to objective conditions [13]. In cases of telecommunications and online fraud, victims are often spread across the country or even abroad, and the electronic data and transaction records involved are often in the tens of thousands or even millions. If the investigation authorities are required to verify each piece of evidence one by one, it will not only consume a large amount of human and material resources, but also may lead to the loss of evidence due to the long collection period, affecting the timely investigation and handling of the case. In practice, the determination of necessity requires a comprehensive judgment based on the scale of evidence and the status of judicial resources in specific cases. For example, relevant normative documents in Zhejiang Province clearly state that sampling for evidence collection can be considered when the number of victims reaches 100 [14].

Homogeneity is the essential prerequisite for the application of sampling evidence collection, which requires that the sampled evidence be consistent in type, source and purpose of proof. Homogeneous evidence typically refers to evidence formed when the same criminal gang implements the same fraud scheme, such as a uniform template of fraud script. For the determination of homogeneity of verbal evidence, the narrative structure framework of the fraud case can be used to distinguish the functional differences of the victim's statement in proving the means of the crime, and to ensure the representativeness of the sample through stratified sampling; For physical evidence, it is necessary to examine the uniformity of its storage format and associated objects to avoid distorted sampling conclusions due to heterogeneity of evidence.

Feasibility is the technical prerequisite for the application of sampling evidence. From a technical perspective, the authorities involved in the case need to master basic sampling statistics methods, be able to determine reasonable sampling methods based on the total amount of evidence, and ensure that the samples are sufficiently representative. For complex and massive data, technical support from third-party professional institutions can also be utilized to enhance the scientific nature of sampling through big data analysis methods. From a procedural perspective, the implementation of sampling and evidence collection must comply with legal procedural requirements to ensure the openness and traceability of sampling operations. But in practical application, the feasibility judgment also needs to take into account the differences in regional investigation levels. The eastern coastal areas, relying on their well-developed technical systems and talent reserves, have formed mature sampling and evidence collection models. For example, Shanghai, Zhejiang and other places have built professional electronic data forensics laboratories equipped with big data analysis systems, which can achieve automated stratified sampling of tens of millions of electronic data. The sampling error is controlled within 5%; In some western regions, due to insufficient investment in technology, the coverage rate of professional forensic equipment is less than 30%, the proportion of professional technicians is less than 15%, and most of the samples are screened manually. The

DOI: 10.54254/2753-7048/2026.33331

sampling ratio is often less than 1%, and some cases have insufficient sample representativeness due to the lack of scientific verification. This shortcoming should be addressed through cross-regional collaboration, technical support, etc.

3. The theoretical basis of sampling and evidence collection for telecommunications and online fraud

The legitimacy of sampling evidence collection for telecommunications and Internet fraud is mainly rooted in three core theoretical foundations: statistical principles, litigation efficiency theory, and criminal proof standard theory, providing a solid theoretical support for the normative application of sampling evidence collection.

Statistical principles are the scientific basis of sampling and evidence collection. The law of large numbers reveals a positive correlation between sample size and conclusion reliability, that is, as the sample size increases, the sample characteristics will gradually approach the overall characteristics, and the sampling error will decrease and stabilize accordingly. The central limit theorem further explains that regardless of the distribution pattern of the overall evidence, when the sample size is large enough, the sample mean will present a normal distribution, which provides the possibility for the quantitative calculation and control of sampling error. In cases of telecom fraud, the application of these principles enables law enforcement agencies to effectively verify massive amounts of evidence with a small sample size while controlling errors through scientific sampling design.

The theory of litigation efficiency provides a value basis for the application of sampling evidence collection, and its core lies in achieving the optimal allocation of judicial resources. By focusing on key samples, it significantly reduces the workload of evidence collection, review and cross examination, concentrating judicial resources on the verification of core facts. From the perspective of law and economics, sampling for evidence provides a relatively accurate determination of the facts of a case at the lowest cost of evidence collection, in line with the efficiency principle of "obtaining the maximum litigation benefit with the minimum judicial input".

The criminal standard of proof theory provides a normative basis for the proof effect of sampling evidence collection, clarifying that sampling evidence collection does not lower the standard of proof, but rather achieves the compliance of the standard of proof through scientific methods. China's criminal proceedings require "the facts of the case are clear and the evidence is solid and sufficient", and this standard has not loosened in sampling evidence collection. Sampling and evidence collection, through the scientific selection of samples and error control, ensure that the conclusions are reliable enough to meet the proof requirements of excluding reasonable doubt. In practice, the sampling conclusion is not used alone as the basis for determining a case, but needs to be corroborated with other evidence to form a complete chain of evidence.

4. The current situation and predicaments of the practice of sampling evidence collection for telecommunications and Internet fraud

4.1. The current situation of practical operation

According to empirical research, in information network crime cases involving sampling evidence collection, cases related to telecommunications network fraud account for a significant proportion. The types of evidence involved are mainly electronic data and victim statements, both of which account for more than 40 percent in sampling evidence collection cases and become the core applicable objects of sampling evidence collection.

DOI: 10.54254/2753-7048/2026.33331

In terms of application patterns, a pattern of concurrent probability sampling and non-probability sampling has already been formed in practice. Take the case of Zhang Kaimin Telecom Network fraud as an example. In this case, Zhang Kaimin and 52 others set up dens in Indonesia, Kenya and other places and carried out fraud against residents of the Chinese mainland. The amount involved was as high as 23 million yuan and there were 75 victims [15]. Faced with the difficulty of obtaining evidence across the criminal chain, the judicial authorities adopted a compound sampling model for evidence collection. At the level of probability sampling, the law enforcement authorities fully restored and conducted "untainted identification" of the vast amount of electronic data extracted from the computers and mobile phones involved in the case, such as Skype chat records and Excel documents. By using technical means to randomly extract key information nodes from the massive data, the previous fraud facts of the suspects in Indonesia were verified, and 11 suspects who were overlooked were brought to justice. At the non probability sampling level, when collecting statements from victims, the judicial authorities did not mechanically pursue individual evidence collection, but combined objective evidence such as bank account transaction records and call records to comprehensively determine the number of victims and the amount of money defrauded. By focusing on verifying victims whose funds were flowing clearly and whose evidence was complete, a connection was established between the fraud and the consequences of the crime, and ultimately an evidence system was formed, which led to the conviction of 50 defendants. This case clearly shows that in judicial practice, probability sampling and non-probability sampling are not mutually exclusive but are flexibly used according to the type of evidence to jointly build the evidence foundation for combating crime.

4.2. The dilemma of normative operation

4.2.1. Improper sampling procedures, questionable probative force

First, the inherent flaws in the procedure design led to the lack of rigid constraints throughout the sampling operation. Looking at several cases of mass economic crimes, it can be found that the normative implementation of sampling and evidence collection in telecommunications and online fraud cases has always been limited by the inherent deficiencies of procedural design and the subjective arbitrariness of substantive operations. In the absence of clear operational guidelines, investigators conduct sampling based solely on their experience in handling cases, making it difficult to effectively restrain the entire process from initiation to implementation of sampling and evidence collection, thereby greatly reducing the probative force of the substantive samples. The procedural norms for sampling and evidence collection have not yet formed a unified standard. In practice, investigation authorities have shown obvious arbitrariness in the selection of carriers and process records of sampling operations. Some cases simply summarize the sampling behavior with "situation description", some cases make records but lack the core operational elements, and some cases only mark the description of sampling and evidence collection without retaining any operational details. This "black box" operation mode makes the process of generating sampling evidence lose traceability, and the lack of procedural justice directly affects the legitimacy basis of the evidence.

Secondly, the absence of sample size and error rules weakens the overall relevance of the sample. The confusion in the procedures also extended to the substantive level. The current norms only generally require samples to be selected in a certain proportion or quantity, without setting sample size standards and error control rules in light of the characteristics of telecommunications and online fraud cases. Investigators often subjectively determine a sampling ratio far below the reasonable

DOI: 10.54254/2753-7048/2026.33331

range among millions of victims and data information. The correlation between the sample and the whole has been greatly reduced.

Finally, the imbalance in method adaptability makes it difficult to guarantee the proof value. The structure of evidence that combines verbal evidence and electronic data in telecommunications and Internet fraud cases requires the sampling method to be compatible with the type of evidence. However, in practice, investigators blindly apply non-probability sampling, which has a lower operational threshold, to the determination of core facts, making the sample unable to objectively reflect the overall situation of the case and significantly reducing the substantive proof value. Ultimately, it leads to a double dilemma of unregulated procedures and unscientific substance in evidence collection.

4.2.2. The defense is weak in cross-examination and there is an imbalance between the prosecution and the defense

First of all, due to the inherent gap between the prosecution and the defense in their ability to obtain evidence and their professional technical level, there is a reality that the exercise of the right to cross-examine is unbalanced and the effect is weakened. The professionalism and concealment of sampling and evidence collection further magnify the passive position of the defense in cross-examination, making it difficult for the cross examination stage to function. The prosecution, as the implementing entity of sampling and evidence collection, holds the full process information of sampling and, relying on investigation resources and professional techniques, has an absolute information advantage in cross-examination. In the case of telecommunications and online fraud, the defense lacks access to the vast amount of data involved in the case, nor does it have the statistical expertise and technical means required for sampling and evidence collection. Faced with the sampling evidence submitted by the prosecution, it is difficult to raise substantive questions from a professional perspective.

Secondly, and more importantly, the sampling process in telecommunications and Internet fraud cases often follows the principle of investigation confidentiality. The investigation authorities have not fully disclosed the details of the sampling to the defense, and the materials that the defense can obtain are only the sampling conclusions screened by the prosecution, unable to effectively review the source and process of the sampling. When the defense raises objections regarding the number of samples and the method of selection, courts often ignore the defense's cross examination opinions on the grounds of the legality of sampling under objective conditions, and even covertly require the defense to provide reverse sampling conclusions to support the doubts, undoubtedly increasing the defense's burden of proof. Finally, the prosecution does not need to provide detailed explanations of every step of the sampling process during the cross examination, and the defense's cross-examination lacks substantive facts and professional support, resulting in the cross-examination of sampling evidence in telecommunications and online fraud cases being merely formal, the defense's right to cross-examination is difficult to be truly implemented, and the imbalance of cross-examination between the prosecution and the defense becomes an important obstacle to the standardized operation of sampling evidence.

4.2.3. The absence of review rules and subjective assumptions in certification judgments

First of all, in the certification process of sampling evidence in telecommunications and online fraud cases by judges, due to the lack of clear review rules and determination standards, there are subjective assumptions in the judgment of evidential capacity and probative force. The judges' lack

DOI: 10.54254/2753-7048/2026.33331

of professional knowledge and the absence of review rules make it difficult to guarantee objectivity and uniformity in the certification results of the sampled evidence. The current norms do not set specific review requirements for the legality of sampling and evidence collection procedures. When judges determine whether sampling evidence has evidentiary capacity, they simply review whether it meets the formal requirements of "particularly large quantity" and "objective conditions limit that it cannot be collected one by one", and the review of procedural elements such as the approval authorization and document production of sampling is superficial. Even if there are obvious procedural flaws in the sampling operation in some cases, it is often determined to have evidentiary capacity due to the difficulty in obtaining objective evidence, and the restrictive effect of procedural legality on evidentiary capacity is greatly weakened.

Secondly, judges are mostly "outsiders" in the field of statistics and are unable to conduct professional reviews of the confidence intervals and error calculations of probability sampling, as well as the selection basis of non probability sampling. They can only make subjective judgments based on the unilateral explanations of the prosecution and their own experience in handling cases. At the same time, the current norms do not establish a hierarchical probative force review rule, do not distinguish the differences in probative force between probability sampling and non-probability sampling, and do not specify the requirements for corroboration of sampling evidence with other evidence on record. Judges often directly use the sampling conclusion as the basis for determining the facts of the case in certification, ignoring the auxiliary characteristics of sampling evidence. Even when there is a contradiction between the sampling evidence and other evidence, the sampling conclusion is still given priority for acceptance. Finally, judges in different regions have significant differences in the scrutiny standards for sampled evidence of telecommunications and online fraud. Some courts have strict requirements for the professional details of the sampling, while others only conduct formal reviews. This certification model, lacking a unified review rule, makes the determination of the probative force of sampled evidence highly subjective and speculative, affecting the accuracy of the determination of facts in cases.

5. The standardized operation path of sample evidence collection for telecommunications and Internet fraud

5.1. Standardize sampling operations and lay a solid scientific foundation for evidence collection

First, in response to procedural loopholes in the evidence collection process of telecommunications and online fraud cases, a hierarchical sampling approval and authorization mechanism should be established. Investigators should submit a special report stating the necessity of sampling, the basis for judging the homogeneity of evidence, and the proposed sampling method in light of the actual situation such as the number of people involved in the case and the geographical distribution. After preliminary review by the case-handling department and final approval by the person in charge of the public security organ at or above the county level, the sampling operation shall not be initiated without authorization to reduce the randomness of sampling from the source.

Secondly, unify the standards for document production and process recording of sampling and evidence collection, formulate a template for sampling and evidence collection records specifically for telecommunications and Internet fraud cases, and specify that the records should cover core elements such as sampling time and place, total amount of evidence and sample size, information of participants, and the entire sampling process should be supervised by witnesses with a background in statistics who have no interest relationship. After the record is completed, it should be signed and

DOI: 10.54254/2753-7048/2026.33331

confirmed by investigators, witnesses, etc. and uploaded to the case-handling system simultaneously to achieve full traceability of the sampling process and break the drawbacks of the "black box" operation.

Finally, it is necessary to strengthen the training of the sampling professional ability of investigators, regularly conduct special training on statistical knowledge and the practical operation norms of sampling in telecommunications and online fraud cases, promote the transformation of investigators from experience-based sampling to scientific sampling, make the professionalism of sampling operation match the demand for evidence collection in telecommunications and online fraud cases, and consolidate the substantive proof foundation of sample evidence.

5.2. Improve the cross-examination mechanism and balance the litigation positions of both the prosecution and the defense

First, make it clear that the prosecution's obligation to fully disclose the sampling evidence is a prerequisite for the defense to effectively exercise the right of cross-examination. The prosecution not only needs to provide the defense with the sampling conclusion, but also needs to fully disclose all the case file materials of the sampling evidence collection, including the sampling approval documents, operation records and other professional contents, and for the sampling operation involving the statistics profession, there should be a professional interpretation and explanation that is easy to understand. To enable the defense to have a clear understanding of the entire sampling process information.

Secondly, a professional support mechanism for the defense should be established, allowing the defense to hire expert assistants in statistics and network technology to participate in the cross-examination, who can offer professional opinions on issues such as the rationality of the sampling method and the representativeness of the sample, to make up for the defense's deficiencies in professional knowledge and technical ability, and to provide substantive professional support for the cross-examination.

Finally, it is necessary to clarify the rules for the allocation of the burden of proof in the cross-examination stage to reduce the situation of improper transfer of the burden of proof. In the cross-examination of sampling evidence collection in telecommunications and online fraud cases, the prosecution always bears the burden of proof for the legality, relevance and authenticity of the sampling evidence. The defense only needs to raise reasonable doubts about the problems existing in the sampling evidence and provide preliminary evidence. There is no obligation to provide proof of reverse sampling. When the defense raises an objection to the sampling evidence, the court shall require the prosecution to provide a reasonable explanation for the compliance of the sampling operation and corresponding evidence to support it. If the prosecution is unable to provide a reasonable explanation or fails to provide evidence, the court shall exclude the sampling evidence in accordance with the law and make a fact-finding. At the same time, improve the system of sampling personnel appearing in court for cross-examination. If the defense raises substantive objections to the sampling evidence and requests the sampling personnel to appear in court, the court shall notify the relevant investigators to appear in court for questioning in accordance with the law. The personnel appearing in court shall provide detailed explanations on issues such as the specific process of the sampling operation, so that the confrontational and substantive nature of the cross-examination process can be demonstrated. The improvement of the procedure will promote the substantive balance of the litigation status of the prosecution and the defense.

DOI: 10.54254/2753-7048/2026.33331

5.3. Establish hierarchical review rules and standardize judge certification standards

First, in light of the characteristics of telecommunications and online fraud cases, establish hierarchical rules for reviewing the competence of sampling evidence, with procedural legality as the core element of the competence of evidence review. Judges should focus on reviewing procedural elements such as whether the sampling evidence has fulfilled the approval and authorization procedures and whether the witnesses have the corresponding qualifications. For sampling evidence with significant procedural flaws that cannot be corrected, The evidence capacity should be denied to prevent procedural flawed evidence from entering the fact-finding stage of the case. At the same time, clarify the standards for the connection between the formal and substantive requirements of the examination of evidence capacity, examine whether the sampling for evidence collection meets the applicable conditions stipulated in the 2022 Opinion, and in light of the actual situation, provide specific guidance for the determination of "objective condition limitations" to avoid the drawbacks of only conducting formal examination.

Secondly, establish scientific and standardized rules for the review of probative force, distinguishing the standards for the determination of probative force for different sampling methods. For evidence obtained by probability sampling, the judge needs to examine whether the setting of the sample size is reasonable, whether the sampling method conforms to statistical principles, whether the error calculation is scientific, and at the same time, examine whether the sampling evidence is corroborated with other evidence on record. Only when the sampling operation is scientific and standardized and corroborates with other evidence can its higher probative force be confirmed. For verbal evidence obtained by non-probabilistic sampling methods, it is clear that it only has the effect of supporting proof and shall not be used alone as the basis for determining the core facts of the case.

Finally, the certification standards of courts across the country can be unified through case guidance to reduce the situation of different judgments in the same case, so that judges' certification behavior has rules to follow and examples to refer to, and the standardization and unification of the certification standards for sampling evidence of telecommunications and online fraud can be achieved.

6. Conclusion

As an important means to solve the predicament of massive evidence in telecommunications and online fraud, the proper application of sampling evidence affects the fairness and authority of litigation procedures. In current judicial practice, the sampling and evidence collection of telecom and Internet fraud still faces multiple practical predicaments such as improper evidence collection operations and imbalance between prosecution and defense. These problems are not only the shortcomings of the sampling and evidence collection system itself, but also reflect the insufficient compatibility of traditional rules with new types of cyber crimes and other cases. In fact, the standardized operation of sampling and evidence collection is not only an optimization of the technical aspects of investigation and evidence collection, but also involves core propositions such as the implementation of the principle of evidence-based adjudication, the guarantee of equal confrontation between the prosecution and the defense, and the supervision of the operation of judicial power. In the context of the continuous high incidence of telecommunications and Internet fraud cases, short-term policy adjustments and campaign-style governance may have a certain restraining effect, but in the long run, only by establishing a scientific and systematic sampling and evidence collection rule system based on the characteristics and laws of telecommunications and

DOI: 10.54254/2753-7048/2026.33331

Internet fraud crimes can we fundamentally avoid practical chaos and return to the essential requirements of criminal proceedings to safeguard human rights and provide fair justice.

References

[1] Wang Yuting. An empirical Study on Sampling Evidence Collection in Information Network Crime cases [D]. Jilin University, 2024.
[2] Li Yuhua. Research on Criminal Proof Standards [D]. Beijing: China University of Political Science and Law, 2005: 52.
[3] Ma Zhonghong. On Sampling Evidence Collection in Cybercrime Cases: Focusing on Telecommunication Fraud Crimes [J]. Journal of People's Public Security University of China (Social Sciences Edition), 2018(6): 69-78.
[4] Ren Dong. Three levels of Reliability Review of Criminal Sampling Evidence [J]. Evidence Science, 24, 32(4): 405-418.
[5] Liu Xin, Pan Xuening. Problems and responses to the application of criminal sampling proof [J]. Evidence Science, 24, 32(4): 389-404.
[6] Lin Xianrui. The proof mechanism and application rules of criminal sampling evidence collection [J]. Journal of the People's Public Security University of China (Social Sciences Edition), 25, 41(6): 80 90.
[7] Wan Yi, Zong Bo. On Sampling evidence in Criminal proceedings [J]. Journal of Jiangsu Administration Institute, 2014(4): 120-128.
[8] Zheng Fei. On Criminal Sampling Evidence Collection in the Digital Age [J]. Qiushi Academic Journal, 2023(3): 132-141.
[9] Lao Dongyan. Take criminal presumption seriously [J]. Legal Studies, 2007(2): 21-37.
[10] Zheng Fei. The legitimacy and limitations of sampling rules in Information Network crime cases [J]. Journal of Beihang University (Social Sciences Edition), 2023(1): 58-60.
[11] Standing Committee of the National People's Congress. Decision on the Administration of Judicial Expertise (Amended in 2015).
[12] Teng Yuqun. Research on Criminal Sampling in Cybercrime [D]. Zhejiang Gongshang University, 2022.
[13] Zhang Zhuoni. Reflections and Improvements on Sampling Proofs of mass Cybercrime [J]. Journal of Guangxi University (Philosophy and Social Sciences Edition), 24, 46(6): 197-208.
[14] Higher People's Court of Zhejiang Province, People's Procuratorate of Zhejiang Province, Public Security Department of Zhejiang Province. Answers to Several Questions Concerning the Handling of Cases of Telecommunications and Internet Fraud (2020).
[15] The 18th batch of Guiding cases of the Supreme People's Procuratorate: Telecommunication and Internet Fraud Case of Zhang Kaimin et al. (Prosecutor's Case No. 67).